BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11837 A1

(51) International Patent Classification[7]: H04L 12/64

(21) International Application Number: PCT/US00/21587

(22) International Filing Date: 8 August 2000 (08.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/370,504 9 August 1999 (09.08.1999) US

(71) Applicant: MCI WORLDCOM, INC. [US/US]; 515 East Amite Street, Jackson, MI 39201 (US).

(72) Inventors: GALLANT, John, K.; 1800 Azurite Trail, Plano, TX 75075 (US). DONOVAN, Steven, R.; 704 Forest Bend, Plano, TX 75025 (US).

(74) Agent: GROLZ, Edward, W.; Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530 (US).

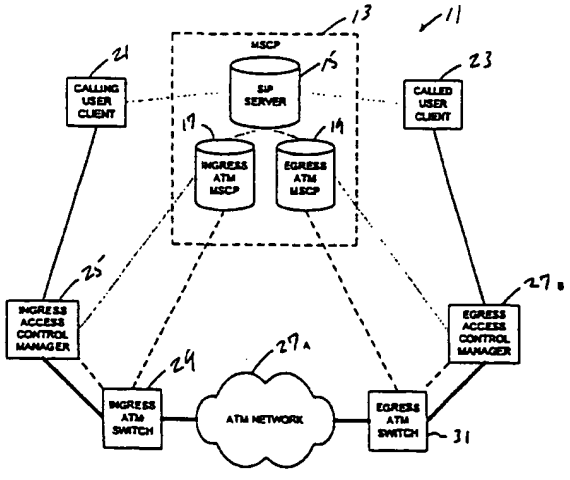
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: METHOD OF AND SYSTEM FOR PROVIDING QUALITY OF SERVICE IN IP TELEPHONY



(57) Abstract: A method and system (11) for providing quality of service in an IP telephony session between a calling party (21) and a called party (23) establishes a high quality of service ATM virtual circuit for the session between first and second devices (25, 27), each of the devices (25, 27) having ATM capability and IP capability. The first and second devices (25, 27) provide bidirectional translation between IP media and ATM media. The system (11) transports IP media for the session between the calling party (21) and the first device (25), and between said called party (23) and a second device (27). The virtual circuit transports ATM media for the session between the first and second devices (25, 27). An intelligent control layer (13) provides IP and ATM signaling to set up the session.

WO 01/11837 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD OF AND SYSTEM FOR PROVIDING QUALITY OF SERVICE IN IP TELEPHONY

The present invention relates generally to the field of Internet telephony, and more particularly to a method of and system for providing quality of service in an Internet telephony session.

Two trends are currently occurring in the telecommunications marketplace. First, telephony services are being added to Internet protocol-based devices. Second, Asynchronous Transfer Mode (ATM) networks are being built with the ability to support user specified quality of service (QoS) on a per connection basis, as part of the ATM switched virtual circuit service capability.

Each of these trends have problems. The primary problem with the introduction of telephony services to the IP network is one providing predictable QoS on a per call/connection basis. Although technologies are being developed in the Internet community to address this problem, there is currently no way to guarantee QoS on a per connection basis through an IP network. The primary problem with the second trend is not one of basic service capability, but is rather one of access to the service. Today virtually all desktop devices have access to an IP network through some sort of local area network technology, for example through Ethernet. The problem is that these desktop devices generally do not have access to ATM networks that provide the per call/connection guarantee QoS.

The primary method of addressing QoS in the current IP-BASED networks is to over-provision the amount of bandwidth available in the network. This approach will work as long as the usage of the network stays within the bounds of the available bandwidth. If the usage of the network is not predictable, then it is difficult, for example, to prevent a low priority file transfer from interfering with a connection established to carry real-time voice or video data.

The primary method of providing ATM switched virtual circuit services to devices that do not have native ATM support is to install routers between the IP network and the ATM network that have the ability to generate ATM switched virtual circuits on a per IP flow basis. The problems with this approach are: (1) possible destination IP addresses need to be provisioned in the router ahead of time, and (2) it is not possible to define, on an IP flow basis, which IP flow should get the ATM switched virtual circuit service and which should get IP best efforts service. If a destination address is provisioned in the ATM interworking router, then all connections to that destination address will require an ATM switched virtual circuit.

The present invention provides a method of and a system for providing quality of service in an IP telephony session between a calling party client and a called party client. The system of the present invention establishes a high quality of service ATM virtual circuit for the session between first and second devices, each of the devices having ATM capability and IP capability. The first and second devices provide bidirectional translation between Internet Protocol (IP) media and ATM media. The system transports IP media for the session between the calling party client and the first device, and between the called party client and the second device. The virtual circuit transports ATM media for the session between the first and second devices. An intelligent control layer provides IP and ATM signaling to set up the session.

In one embodiment of the present invention, the first and second devices include access control managers that are bridges between an IP network and an ATM network. The intelligent control layer assigns a temporary session IP proxy address for the called party at the first access control manager and a temporary session IP proxy address for the calling party at the second access control manager. The system establishes a switched virtual circuit through the ATM network for the session between the first access control manager and the second access control manager by assigning a temporary session calling party number at the first access control manager and a temporary session called party number at the second access control manager.

During the session, the system routes IP media from the calling party to the temporary IP proxy address of the called party at the first access control manager. The first access control manager packages the IP media in ATM cells for transport through the virtual circuit to the second access control manager. The system then routes IP media from the second access control manager to the called party. Similarly, the system routes IP media from the called party to the temporary IP proxy address of the calling party at the second access control manager. The second access control manager packages the IP media in ATM cells for transport through the virtual circuit to the first access control manager. The system then routes IP media from the first access control manager to the calling party.

In an alternative embodiment, the first and second devices include routers that have both IP and ATM capability. The calling party client obtains an authentication ticket and then initiates an IP telephony session with a quality of service request. When the called party client accepts the session, the calling party client initiates setup of a resource reservation protocol IP media session with an ingress router. The ingress router then sets up the IP media session through an egress router to the

called party client. When the IP media session is setup, the ingress router sets up an ATM switched virtual connection with the egress router.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a preferred embodiment of the system of the present invention.

Fig. 2 is a call flow diagram illustrating the signaling and call setup according to the embodiment of Fig. 1.

Fig. 3 is a block diagram of an alternative embodiment of the system of the present invention.

Fig. 4 is a call flow diagram illustrating the signaling and call setup according to the embodiment of Fig. 3.

DETAILED DESCRIPTION

Referring now to the drawings, and first to Fig. 1, a system according to a preferred embodiment of the present invention is designated generally by the numeral 11. System 11 includes a media service control point (MSCP) 13. MSCP 13 includes an IP telephony session establishment server, which in the preferred embodiment is a session initiation protocol (SIP) server 15, an ingress Asynchronous Transfer Mode (ATM) MSCP 17, and an egress ATM MSCP 19. As will be explained in detail hereinafter, MSCP 13 provides an intelligent control layer for the establishment of an Internet Protocol (IP) telephony session between a first IP telephony user client 21 and a second IP telephony user client 23.

System 11 includes an ingress access control manager 25 and an egress access control manager 27. Access control managers 25 and 27 provide a media gateway between IP telephony user clients 21 and 23 and an ATM network 27. Ingress access control manager 25 provides an ATM media and signaling interface to an ingress ATM switch 29 of ATM network 27. Similarly, egress access control manager 27 provides an ATM media and signaling interface to an egress ATM switch 31 of ATM network 27.

In Fig. 1, IP signaling paths are indicated with dotted lines and ATM of signaling paths are indicated with dashed lines. IP media paths are indicated with solid lines and ATM media paths are indicated with bold solid lines.

In the embodiment of Fig. 1, a Quality of Service (QoS) connection is provided by routing traffic on the QoS capable backbone provided by ATM network 27. According to the present

invention, an ATM connection is created for the IP telephony session between user clients 21 and 23. QoS extensions to the data network applications part (DNAP) protocol perform the signaling between MSCP 13 and access control managers 25 and 27. The access control managers 25 and 27 establish the ATM QoS capable connection. While in the preferred embodiment of present invention, the QoS capable connection is provided by ATM switched virtual circuits, the present invention can also be implemented in a variety of other technologies, such as SONET, and wave division multiplexing.

As will be explained in detail hereinafter, the data path for the session is secured against unauthorized traffic by the use of proxy addressing. The proxy addressing requires translation by the access control managers 25 and 27 to route the media to its intended destination. During session establishment, the addresses of the media stream endpoints are exchanged between user client 21 and user client 23. The signaling message containing the media address of user client 21 is changed to reflect a proxy address, which is an interface at egress excess control manager 27. The excess control manager interface is assigned on a per session basis. The per session interface uniqueness is accomplished by the allocation and deallocating of ephemeral ports at the access control managers. Associated with the ephemeral ports are the addresses used to create and transit the ATM connection. Likewise, the signaling message containing the media address for user client 23 is changed to reflect a proxy address at ingress access control manager 25.

The system of the present invention dynamically configures QoS connections and ensures their security in two ways. First, the QoS connection is dynamically configured by the use of ATM switched virtual connections. The switched virtual connections are created on a per session basis during call establishment. MSCP 13 invokes the IP to ATM interface mechanisms of access control managers 25 and 27 with DNAP QoS messages. As will be explained in detail hereinafter, access control manager 25 launches a user network interface (UNI) protocol setup. The ATM traffic sent to and received by access control managers 25 and 27 is intercepted by ATM switches 29 and 31, respectively, and forwarded to their associated ATM MSCPs 17 and 19. The ATM MSCPs create the switched virtual circuit between ATM switches 29 and 31. Access control managers 25 and 27 map the media stream of the session to its switched virtual circuit and the session traffic transits their respective switch virtual circuit.

The second aspect of the real-time configuration solution is the dynamic securing of the access to the connections. This is done by dynamically allocating the proxy addresses during session establishment from a pre-provisioned proxy address pool. The proxy addresses are returned to the

user clients 21 and 23 in the signaling messages. The session proxy address mapping is created at the MSCP and communicated to access control managers 25 and 27 by the DNAP protocol. The proxy addresses and the actual session addresses are held at the SIP server 15 and the access control managers 25 and 27 for the duration of the session. When the session is terminated, proxy addresses are deallocate.

Referring now to Fig. 2, there is shown a call flow diagram of session initiation according to the embodiment of Fig. 1. User client 21 initiates the session by sending a SIP INVITE message 33 to user client 23. For purposes of illustration, the IP address of user client 21 is A@XYZ.COM. The SIP INVITE is addressed to user client 23 at a proxy address at MSCP SIP server 15, which for purposes to illustration is B@XYZ-SIP.COM. The SIP INVITE specifies the audio source as the real IP address of user client 21, and specifies that QoS is requested. Upon receipt of invite 33, SIP server 15 sends an invite 35 to the real IP address of user client 23, at B@XYZ2000.COM. Invite 35 specifies the audio source as a temporary IP proxy address allocated to user client 21 at egress access control manager 27, which for purposes of illustration is A@ACM-Y.COM. If user client 23 accepts the session, user client 23 sends a 200OK SIP response 37 back to SIP SERVER 15, specifying an audio destination as its real IP address. While in the preferred embodiment, SIP IP telephony signaling is used, other IP signaling protocols, such as H.323 may be used.

Upon receipt of response 37, SIP server 15 allocates a call tag, and sends a reserve bandwidth message 39 to ingress ATM MSCP 17. Message 39 specifies the audio destination for the session of as a temporary IP proxy address allocated to user client 23 at ingress access control manager 25. For purposes of illustration, the temporary IP proxy address allocated user client 23 is B@ACM-X.COM. The bandwidth reservation message also identifies the call tag and specifies the called number for the ATM connection as egress access control manager 27.

Upon receipt of bandwidth reservation message 39, ingress ATM MSCP 17 sends a QoS setup request 41 to ingress access control manager 25. Setup request 41 identifies the real source address and proxy source address for user client 21. Setup request 41 also identifies the call tag and the called party number. Ingress ATM MSCP 17 also sends a QoS setup indication message 43 to egress access control manager 27. Setup indication 43 identifies the real destination address and proxy destination address for user client 23, as well as the call tag and the called party number for the ATM session. Egress access control manager 27 responds to setup indication 23 with a setup indication acknowledgment 45 back to ingress ATM MSCP 17. Upon receipt of the QoS setup request 41,

ingress access control manager 25 sends a user network interface (UNI) protocol setup message 47 to ingress ATM switch 29. Upon receipt of UNI setup message 47, ingress ATM switch 29 sends a DNAP setup 49 to ingress ATM MSCP 17. When ingress ATM MSCP 17 responds, as indicated at 51, ingress ATM switch 29 sends a setup message 53 to egress ATM switch 31. Upon receipt of setup message 53, egress ATM switch 31 sends a DNAP setup message 55 to egress ATM MSCP 19. When egress ATM MSCP 19 responds, as indicated at 57, egress ATM switch 31 sends a UNI setup message 59 to egress access control manager 27.

Upon receipt of setup message 59, egress access control manager 27 sends a CONNECT message 61 to ingress access control manager 25. Upon receipt of CONNECT message 61, ingress access control manager 25 responds to QoS setup request 41 with a QoS setup request acknowledgment 63 back to ingress ATM MSCP 17. Upon receipt of setup request acknowledgment 61, ingress ATM MSCP 17 responds to the reserve bandwidth message 39 with a reserve bandwidth acknowledgment message 65 back to MSCP SIP server 15. Upon receipt of reserve bandwidth acknowledgment 65, SIP server 15 deallocate the call tag and sends a SIP 200 OK response 67 back to user client 21. The OK response identifies the audio destination as the temporary IP proxy address allocated to user client 23 at ingress access control manager 25. Then, user client 21 sends IP media packets addressed to user client 23 at the temporary proxy address at access control manager 25. Similarly, user client 23 sends IP media packet addressed to user client 21 at the temporary proxy address at egress access control manager 27.

From the foregoing, it may be seen that the embodiment of Fig. 1 provides QoS for IP telephony sessions between IP user clients. Through the use of temporary proxies, user clients 21 and 23 are unaware that their session is carried on an ATM switched virtual circuit. User clients 21 and 23 use standard SIP messaging and standard proxying for call setup and no special intelligence is required on the part of the user clients 21 and 23. An intelligent network layer makes the system of the present invention transparent to user clients 21 and 23.

Referring now to Fig. 3, an alternative embodiment of the system of the present invention is designated generally by the numeral 71. System 71 includes MSCP indicated generally at 73. MSCP 73 includes an MSCP SIP server 75, an ingress ATM MSCP 77, and an egress ATM MSCP 79. Additionally, MSCP 73 includes a policy server 81. MSCP 73 is adapted to establish a QoS IP telephony session between a calling user client 83 and a called user client 85.

An ingress router 87 provides an interface between IP user client 83 and an ATM network 89.

An egress router 91 provides interface between user client 85 and ATM network 89. Ingress router 87 provides an interface to an ingress ATM switch 93 of ATM network 89. Similarly, egress router 91 provides an interface to an egress ATM switch 95 of ATM network 89.

Referring now to Fig. 4, there is shown a call flow diagram of session initiation according to the enbodiment of Fig. 3. User client 83 initiates the session with a Diameter protocol session authentication request 97 addressed to MSCP SIP server 75. Server 75 responds with a Diameter session authentication response (ticket), as indicated at 99. Then, user client 83 sends a SIP INVITE message 101 to user client 85. For purposes of illustration, the IP address of user client 85 is A@XYZ.COM. The SIP INVITE 101 is addressed to user client 85 at a proxy address at MSCP SIP server 75, which for purposes to illustration is B@XYZ-SIP.COM. The SIP INVITE 101 specifies the audio source as the real IP address of user client 83, and specifies that QoS is requested. The SIP INVITE 101 also includes the authentication ticket received in response to Diameter session authentication request 97. Upon receipt of the SIP INVITE 101, SIP server 75 sends an INVITE 103 to the real IP address of user client 85, at B@XYZ2000.COM. INVITE 103 specifies the audio source as the IP address of user client 83. If user client 85 accepts the session, user client 85 sends a 200OK SIP response 105 back to SIP Server 75, specifying an audio destination as its real IP address.

Upon receipt of 200OK SIP response 105, SIP server 75 sends a reserve bandwidth message 107 to MSCP policy server 81. Message 107 specifies the audio source for the session of as the real IP address of user client 83, and the audio destination for the session as the real IP address of user client 85. The message 107 also includes the authentication ticket. Upon receipt of the message 107, MSCP policy server 81 sends a response 109 back to MSCP SIP server 81. Then, SIP server 75 sends a SIP 200OK response 111 to user client 83.

Upon receipt of 200OK response 111, user client 83 sends a resource reservation protocol (RSVP) path message 113 to ingress router 87. Then, ingress router 87 sends a COPS request handle message 115 to MSCP policy server 81. When MSCP policy server 81 responds, as indicated at 117, ingress router 87 sends an RSVP path message 119 to egress router 91. Then, egress router 91 sends an RSVP path message 121 to user client 85. User client 85 responds with an RSVP reservation response 123 back to egress router 91. Egress router 91 then responds with an RSVP reservation response 125 back to ingress router 87.

Upon receipt of response 125, ingress router 87 sends a UNI setup message 127 to ingress ATM switch 93. Upon receipt of UNI setup message 127, ingress ATM switch 93 sends a DNAP

setup 129 to ingress ATM MSCP 77. When ingress ATM MSCP 77 responds, as indicated at 131, ingress ATM switch 93 sends a setup message 133 to egress ATM switch 95. Upon receipt of setup message 133, egress ATM switch 95 sends a DNAP setup message 135 to egress ATM MSCP 79. When egress ATM MSCP 79 responds, as indicated at 137, egress ATM switch 95 sends a UNI setup message 139 to egress router 91.

Upon receipt of setup message 139, egress router 91 sends a CONNECT message 141 to ingress router 87. Upon receipt of CONNECT message 141, ingress router 87 responds to RSVP path message 113 with an RSVP reserve response 143 back to user client 83. Then, the IP telephony session is established between user client 83 and user client 85.

The embodiment of Figs. 3 and 4, distributes a certain amount of system intelligence to user clients 83 and 85. User clients 83 and 85 are responsible for a greater part of call setup than are user clients 21 and 23 of the embodiment of Figs. 1 and 2. User clients 83 and 85 process signaling in Diameter and RSVP protocols in addition to signaling in SIP protocol.

From the foregoing it may be seen that the present invention overcomes the shortcomings of the prior art. The present invention dynamically establishes and secures QoS IP telephony sessions by routing traffic on a high QoS backbone, which is preferably an ATM backbone. Those skilled in the art will recognize alternative embodiments, given the benefit of this disclosure. Accordingly, the foregoing disclosure is intended for purposes of illustration and not limitation.

WHAT IS CLAIMED IS:

1. A method of providing quality of service in an Internet Protocol (IP) telephony session between a calling party and a called party, which comprises the steps of:

transporting IP media for said session between said calling party and a first device having IP capability and ATM capability;

transporting IP media for said session between said called party and a second device having IP capability and ATM capability; and

establishing an ATM virtual circuit for said session between said first device and said second device.

2. The method as claimed in claim 1, wherein said first and second devices are routers.

3. The method as claimed in claim 1, wherein:

said first device is identified by a temporary session IP proxy address for said called party; and

said second device is identified by a temporary session IP proxy address for said calling party.

4. The method as claimed in claim 1, wherein said step of establishing an ATM virtual circuit between said first and second devices comprises the steps of:

assigning a calling party number for said session at said first device; and

assigning a called party number for said session at said second device.

5. A method of providing quality of service in an IP telephony session between a calling party and a called party, which comprises the steps of:

assigning a temporary IP proxy address for said called party for said session at a first access control manager;

assigning a temporary IP proxy address for said calling party for said session at a second access control manager; and

establishing a switched virtual circuit for said session between said first access control manager and said second access control manager.

6. The method as claimed in claim 5, wherein said step of establishing said virtual circuit comprises the steps of:

assigning a temporary calling party address for said session at said first access control manager; and

assigning a temporary called party address for said session at said first access control manager.

7. The method as claimed in claim 6, wherein said step of assigning a temporary calling party address comprises the step of selecting a calling party address from a pool of calling party addresses allocated to said first access manager.

8. The method as claimed in claim 6, wherein said step of assigning a temporary called party address comprises the step of selecting a called party address from a pool of called party addresses allocated to said second access manager.

9. The method as claimed in claim 5, further comprising the steps of:

routing IP media traffic from said calling party to said called party IP proxy address at said first access control manager; and

routing IP media traffic from said called party to said calling party IP proxy address at said second access control manager.

10. The method as claimed in claim 9, further comprising the steps of:

translating IP media traffic received at said called party IP proxy address to ATM traffic for transport through said virtual circuit from said first access control manager to said second access control manager; and

translating IP media traffic received at said calling party IP proxy address to ATM traffic for transport through said virtual circuit from said second access control manager to said first access control manager.

11. The method as claimed in claim 10, further comprising the steps of:

translating ATM traffic received at said temporary called party address to IP media traffic for transport to said called party; and

translating ATM traffic received at said temporary calling party address to IP media traffic for transport to said calling party.

12. A method of providing quality of service in an IP telephony session between a calling party and a called party, which comprises the steps of:

assigning a temporary IP proxy address for said called party for said session at a first access control manager;

assigning a temporary IP proxy address for said calling party for said session a second access control manager;

assigning a temporary second network calling party address for said session at said first access control manager; and

assigning a temporary second network called party address for said session at said first access control manager.

13. The method as claimed in claim 12, wherein said step of assigning a temporary second network calling party address comprises the step of selecting a calling party address from a pool of second network calling party addresses allocated to said first access manager.

14. The method as claimed in claim 12, wherein said step of assigning a temporary second network called party address comprises the step of selecting a called party address from a pool of second network called party addresses allocated to said second access manager.

15. The method as claimed in claim 12, further comprising the steps of:

routing IP media traffic from said calling party to said called party IP proxy address at said first access control manager; and

routing IP media traffic from said called party to said calling party IP proxy address at said second access control manager.

16. The method as claimed in claim 15, wherein:

said second network includes an ATM network;

said temporary second network calling party address includes a temporary calling party number; and

said temporary second network called party address includes a temporary called party number.

17. The method as claimed in claim 16, further comprising the step of establishing a switched virtual connection through said ATM network between said temporary called party number and said temporary calling party number.

18. The method as claimed in claim 17, further comprising the steps of:

translating IP media traffic received at said called party IP proxy address to ATM traffic for transport through said virtual circuit from said first access control manager to said second access control manager; and

translating IP media traffic received at said calling party IP proxy address to ATM traffic for transport through said virtual circuit from said second access control manager to said first access control manager.

19. The method as claimed in claim 17, further comprising the steps of:

translating ATM traffic received at said temporary called party number to IP media traffic for transport to said called party; and

translating ATM traffic received at said temporary calling party number to IP media traffic for transport to said calling party.

20. A system for providing a quality of service IP telephony session between a calling party and a called party, which comprises:

an IP network, said IP network providing IP access to the calling party and to the called party;

an ATM network;

a first device connected between said IP network and said ATM network, said first device providing bidirectional translation between IP media traffic and ATM traffic;

a second device connected between said IP network and said ATM network, said second device providing bidirectional translation between ATM traffic and IP media traffic; and

an intelligent control layer for establishing a virtual circuit through said ATM network for an IP telephony session between the calling party and the called party.

21. The system as claimed in claim 20, wherein:

said first device is operably connected to an ingress switch of said ATM network; and

said second device is operably connected to an egress switch of said ATM network.

22. The system as claimed in claim 20, wherein said intelligent control layer comprises:

an ATM intelligent controller, said ATM intelligent controller providing session setup signaling to said first and second devices; and

an IP intelligent controller, said IP intelligent controller providing call setup signaling to said ATM intelligent controller.

23. The system as claimed in claim 20, wherein in said first and second devices each comprise a router.

24. The system as claimed in claim 20, wherein said intelligent control means comprises:

means for assigning a temporary IP session proxy address for said called party at said first device; and

means for assigning a temporary IP session proxy address for said calling party at said second device.

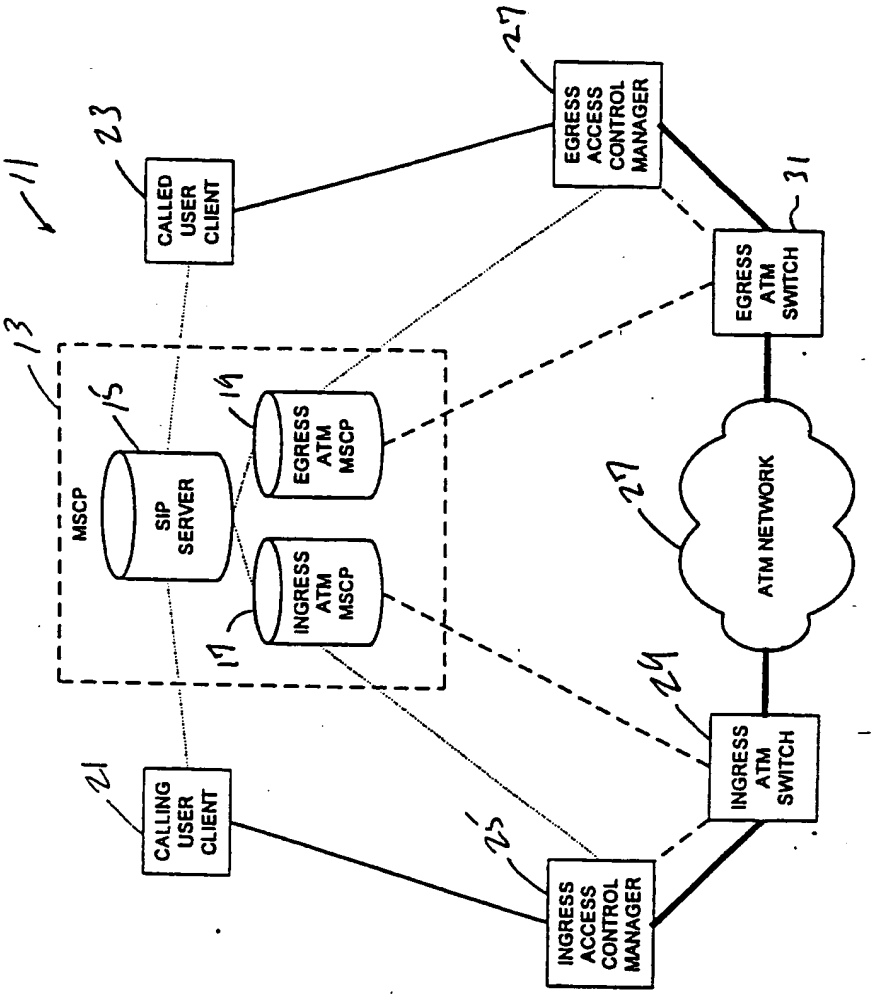

11
13
MSCP
15
SIP SERVER
19
INGRESS ATM MSCP
17
EGRESS ATM MSCP
23
CALLED USER CLIENT
21
CALLING USER CLIENT
27
EGRESS ACCESS CONTROL MANAGER
25
INGRESS ACCESS CONTROL MANAGER
31
EGRESS ATM SWITCH
29
INGRESS ATM SWITCH
27
ATM NETWORK

FIG. 1

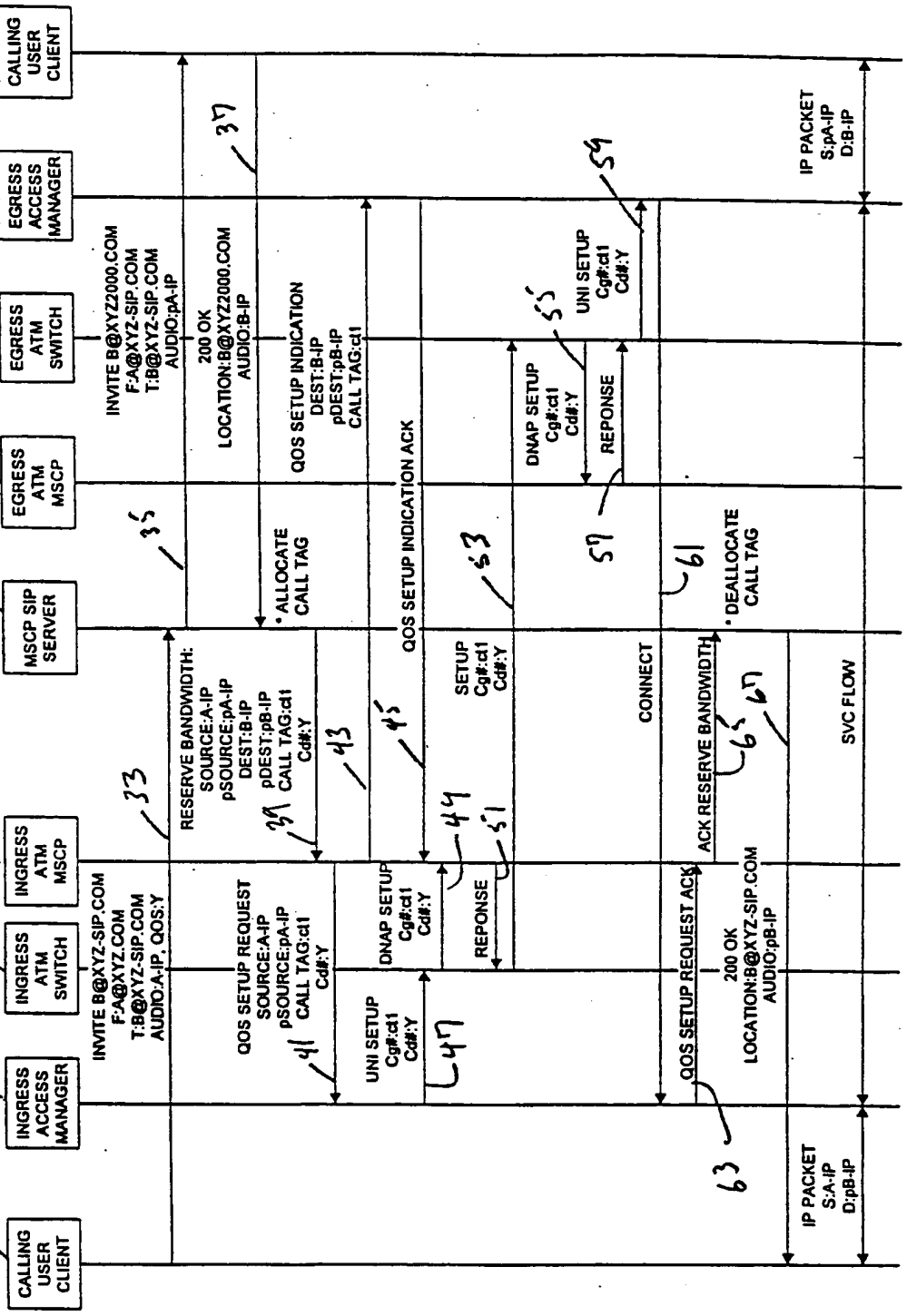

CALLING USER CLIENT
INGRESS ACCESS MANAGER
INGRESS ATM SWITCH
INGRESS ATM MSCP
MSCP SIP SERVER
EGRESS ATM MSCP
EGRESS ATM SWITCH
EGRESS ACCESS MANAGER
CALLING USER CLIENT
INVITE B@XYZ-SIP.COM F:A@XYZ.COM T:B@XYZ-SIP.COM AUDIO:A-IP, QOS:Y
QOS SETUP REQUEST SOURCE:A-IP pSOURCE:pA-IP CALL TAG:d1 Cd#:Y
UNI SETUP Cg#:d1 Cd#:Y
DNAP SETUP Cg#:d1 Cd#:Y
REPONSE
RESERVE BANDWIDTH: SOURCE:A-IP pSOURCE:pA-IP DEST:B-IP pDEST:pB-IP CALL TAG:d1 Cd#:Y
INVITE B@XYZ2000.COM F:A@XYZ-SIP.COM T:B@XYZ-SIP.COM AUDIO:pA-IP
200 OK LOCATION:B@XYZ2000.COM AUDIO:B-IP
• ALLOCATE CALL TAG
QOS SETUP INDICATION DEST:B-IP pDEST:pB-IP CALL TAG:d1
QOS SETUP INDICATION ACK
SETUP Cg#:d1 Cd#:Y
DNAP SETUP Cg#:d1 Cd#:Y
REPONSE
UNI SETUP Cg#:d1 Cd#:Y
CONNECT
• DEALLOCATE CALL TAG
ACK RESERVE BANDWIDTH
QOS SETUP REQUEST ACK
200 OK LOCATION:B@XYZ-SIP.COM AUDIO:pB-IP
SVC FLOW
IP PACKET S:A-IP D:pB-IP
IP PACKET S:pA-IP D:B-IP
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51
53
55
57
59
61
63
65
67

FIG. 2

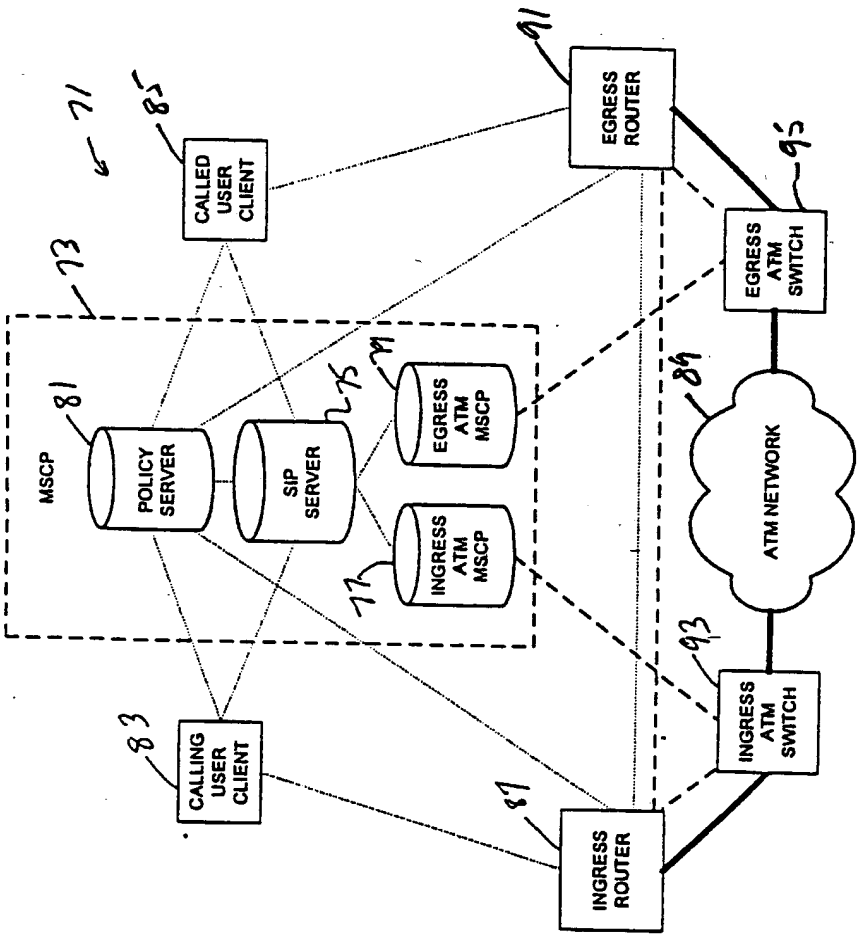

71
85
CALLED USER CLIENT
91
EGRESS ROUTER
95
EGRESS ATM SWITCH
73
MSCP
81
POLICY SERVER
75
SIP SERVER
EGRESS ATM MSCP
INGRESS ATM MSCP
77
84
ATM NETWORK
93
INGRESS ATM SWITCH
83
CALLING USER CLIENT
INGRESS ROUTER

FIG. 3

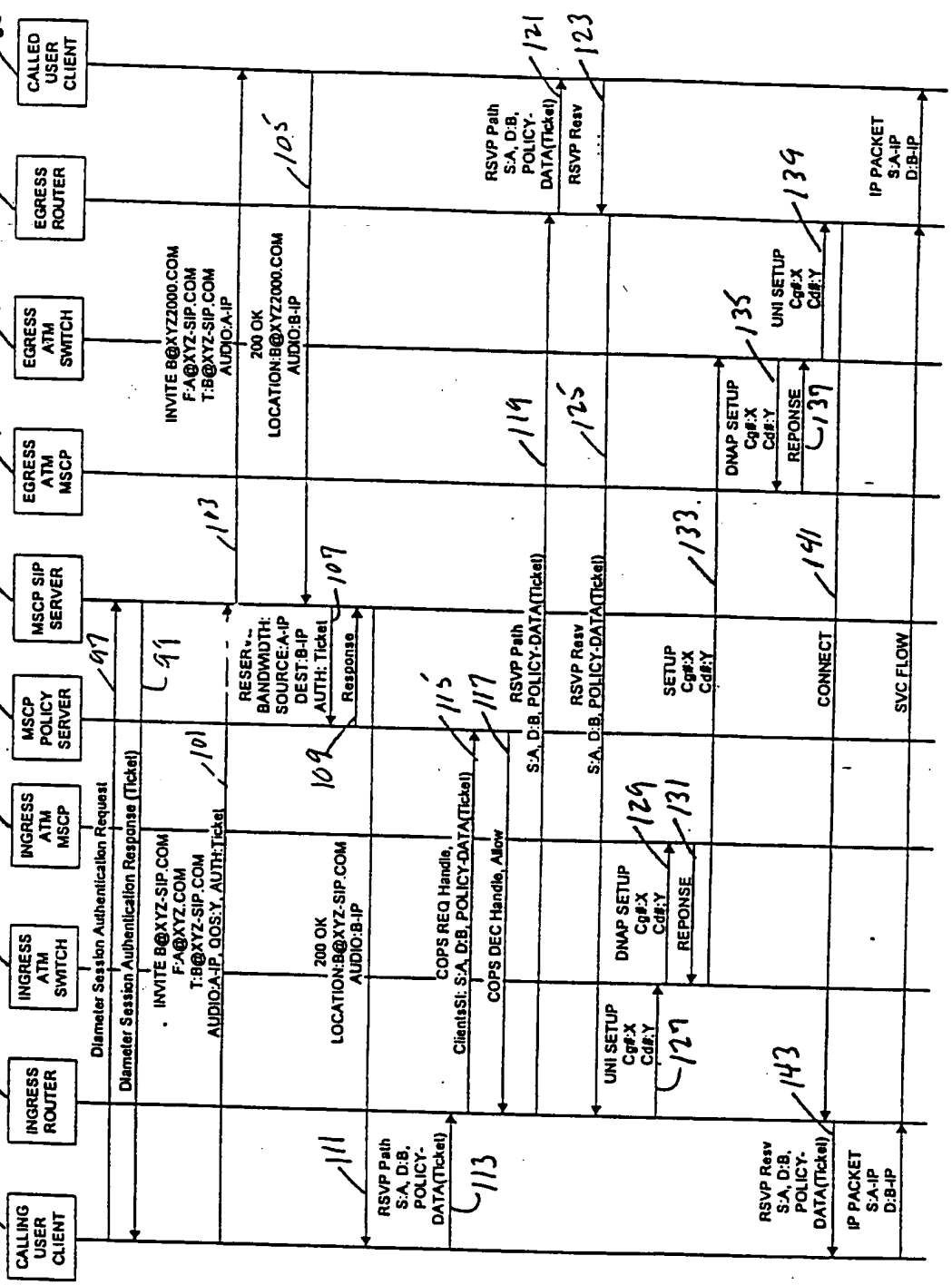

CALLING USER CLIENT
INGRESS ROUTER
INGRESS ATM SWITCH
INGRESS ATM MSCP
MSCP POLICY SERVER
MSCP SIP SERVER
EGRESS ATM MSCP
EGRESS ATM SWITCH
EGRESS ROUTER
CALLED USER CLIENT
Diameter Session Authentication Request
Diameter Session Authentication Response (Ticket)
INVITE B@XYZ-SIP.COM F:A@XYZ.COM T:B@XYZ-SIP.COM AUDIO:A-IP, QOS:Y, AUTH:Ticket
200 OK LOCATION:B@XYZ-SIP.COM AUDIO:B-IP
RESER... BANDWIDTH: SOURCE:A-IP DEST:B-IP AUTH: Ticket
Response
COPS REQ Handle, ClientSI: S:A, D:B, POLICY-DATA(Ticket)
COPS DEC Handle, Allow
RSVP Path S:A, D:B, POLICY-DATA(Ticket)
RSVP Resv S:A, D:B, POLICY-DATA(Ticket)
INVITE B@XYZ2000.COM F:A@XYZ-SIP.COM T:B@XYZ-SIP.COM AUDIO:A-IP
200 OK LOCATION:B@XYZ2000.COM AUDIO:B-IP
RSVP Path S:A, D:B, POLICY-DATA(Ticket)
RSVP Resv ...
UNI SETUP Cg#:X Cd#:Y
DNAP SETUP Cg#:X Cd#:Y
REPONSE
SETUP Cg#:X Cd#:Y
CONNECT
UNI SETUP Cg#:X Cd#:Y
DNAP SETUP Cg#:X Cd#:Y
REPONSE
SVC FLOW
RSVP Path S:A, D:B, POLICY-DATA(Ticket)
RSVP Resv S:A, D:B, POLICY-DATA(Ticket)
IP PACKET S:A-IP D:B-IP
IP PACKET S:A-IP D:B-IP
83
87
93
77
81
75
79
95
91
85
101
103
105
107
109
111
113
115
117
119
121
123
125
127
129
131
133
135
137
139
141
143

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/21587

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 12/64

US CL :370/352, 358, 395, 401, 466; 379/230

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/352, 355, 356, 358, 395, 401, 465, 466, 467; 379/230

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,867,571 A (BORCHERING) 02 February 1999, col. 2, line 45 - col. 3, line 61.	1-24
A	US 5,903,559 A (ACHARYA et al) 11 May 1999, abstract.	1-24
A	US 5,933,412 A (CHOUDHURY et al) 03 August 1999, abstract.	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 02 OCTOBER 2000	Date of mailing of the international search report 24 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer RICKY QUOC NGO Telephone No. (703) 305-4395

Form PCT/ISA/210 (second sheet) (July 1998) *

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31829 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US00/41389

(22) International Filing Date: 20 October 2000 (20.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/160,560 20 October 1999 (20.10.1999) US
09/547,776 12 April 2000 (12.04.2000) US

(71) Applicant: ALCATEL INTERNETWORKING, INC. [US/US]; 26801 West Agoura Road, Calabasas, CA 91301 (US).

(72) Inventors: MARTIN, Christopher; 4404 Becton Court, Apex, NC 27502 (US). EDGINTON, D., Brian; 2675 West 6865 South, West Jordan, UT 84084 (US).

(74) Agent: JEON, Jun-Young, E.; Christie, Parker & Hale, LLP, 350 West Colorado Boulevard, P.O. Box 7068, Pasadena, CA 91109-7068 (US).

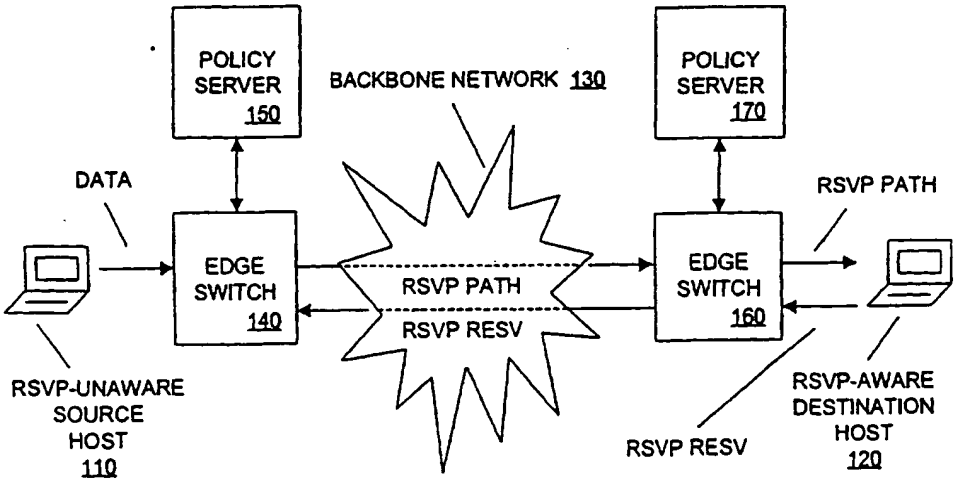
(81) Designated States *(national)*: CN, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: RSVP PROXY SERVICE FOR COMMUNICATION NETWORK



(57) Abstract: RSVP host proxy services for extending RSVP-signaled QoS provisioning to flows involving one or more RSVP-unaware hosts. In an RSVP sender host proxy service, a switch through which an RSVP-unaware source host accesses a network acts as an RSVP sender host proxy for the source host. In an RSVP receiver host proxy service, a switch through which an RSVP-unaware destination host accesses a network acts as an RSVP receiver host proxy for the destination host.

WO 01/31829 A2

RSVP PROXY SERVICE FOR COMMUNICATION NETWORK

BACKGROUND OF THE INVENTION

Data communication switches are becoming more and more intelligent. Whereas legacy data communication switches provided indiscriminate first-in, first-out forwarding of packets, more recent data communication switches support differential packet forwarding based on flow characteristics under the Quality of Service (QoS) label. The trend toward QoS started first in cell-switched ATM networks, but has migrated to packet-switched networks and protocols, including bridging (Layer 2, or "L2"), routing (Layer 3. or "L3") and transport (Layer 4, or "L4") protocols.

Standardized QoS elements are emerging in packet switched networks. One standard element is a signaling protocol through which a QoS may be provisioned end-to-end for a flow. This signaling protocol is called the Resource Reservation Protocol (RSVP). In conventional RSVP-signaled QoS provisioning, an RSVP-aware source host. called a "sender", desiring to initiate a flow with an RSVP-aware destination host. called a "receiver". transmits downstream an RSVP Path message specifying parameters for a proposed flow. Switches along the flowpath review the RSVP Path message and modify certain message fields as required to indicate limitations and conditions on their ability to deliver QoS services to the flow. The RSVP-aware destination host receives the RSVP Path message and uses the information therein to generate and transmit an RSVP Resv message back upstream requesting the provisioning of a specific QoS for the flow at each switch along the flowpath. Each switch determines whether or not to accept the request based on whether the switch has sufficient available resources to provide the requested QoS and whether the flow is entitled to the requested QoS. If the reservation is accepted, the switches are configured to forward packets within the flow in accordance with the QoS. In this way, an RSVP-signaled QoS for the flow is provisioned end-to-end along the flowpath.

While standard RSVP-signaled QoS, as outlined above, provides a means for end-to-end QoS provisioning within a network, it is only known to be available for flows between hosts that are RSVP-aware. There is a need to extend the benefits of RSVP-signaled QoS to flows involving RSVP-unaware hosts.

SUMMARY OF THE INVENTION

The present invention provides RSVP host proxy services for extending RSVP-signaled QoS provisioning to flows involving hosts that are not RSVP-aware.

In accordance with an RSVP sender host proxy service, a switch through which a first host accesses a network acts as an RSVP sender host proxy for the first host. Upon receiving a data packet for a new flow from the first host, and determining that the RSVP sender host proxy service is enabled for the first host. the switch generates and transmits on a flowpath to a second

host an RSVP Path message. In accordance with RSVP, the RSVP Path message prompts the second host to generate and return on the flowpath an RSVP Resv message.

In accordance with an RSVP receiver host proxy service, a switch through which a first host accesses a network acts as an RSVP receiver host proxy for the first host. Upon receiving an RSVP Path message generated and transmitted by a second host and determining that the RSVP receiver host proxy service is enabled for the first host, the switch generates and returns on a flowpath to the second host an RSVP Resv message.

A switch serving as an RSVP host proxy for a host may continue to act as an RSVP router for hosts.

These and other aspects of the inventions may be better understood by reference to the following detailed description taken in conjunction with the accompanying drawings briefly described below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a network in which an RSVP sender host proxy service is operative;

Figure 2 illustrates a switch supporting an RSVP sender host proxy function in the network according to Figure 1;

Figure 3a illustrates the general format for a packet including an RSVP Path message;

Figure 3b illustrates the general format for a packet including an RSVP Resv message;

Figure 4 illustrates a network in which an RSVP receiver host proxy service is operative;

Figure 5 illustrates a switch supporting an RSVP receiver host proxy function in the network according to Figure 4;

Figure 6 is a flow diagram describing RSVP packet handling on a switch supporting an RSVP sender host proxy function in accordance with a preferred embodiment of the invention; and

Figure 7 is a flow diagram describing RSVP packet handling on a switch supporting an RSVP receiver host proxy function in accordance with a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In Figure 1, a network is shown in which a preferred RSVP sender host proxy service in accordance with the invention is operative. The network includes RSVP-unaware source host 110 having access to backbone network 130 via edge switch 140. Edge switch 140 is coupled to edge switch 160 across backbone network 130 via one or more core switches (not shown) operative in backbone network 130. Edge switch 160 is coupled to RSVP-aware destination host 120. Edge switches 140, 160 are also coupled to policy servers 150, 170, respectively.

Hosts 110, 120 are preferably network end-stations, such as PCs, workstations or servers, having respective network interfaces for packetized communication with other hosts via edge switches 140, 160, respectively. Edge switches 140, 160 are preferably gateway devices, such as

hubs, bridges or routers, having a plurality of respective network interfaces for forwarding packetized communications originated by hosts. Policy servers 150, 170 retain quality of service (QoS) rules for application on edge switches 140, 160, respectively, based on flow characteristics. Hosts 110, 120, edge switches 140, 160 and policy servers 150, 170 may be interconnected via cables or other transmission media, and may support various data communication protocols, such as Ethernet, Internet Protocol (IP) and Asynchronous Transfer Mode (ATM). Edge switches 140, 160 preferably support the router function of Resource Reservation Protocol (RSVP) set forth in Internet Engineering Task Force Request for Comment 2205 entitled "Resource ReSerVation Protocol - Version 1 Functional Specification", September 1997 (hereinafter RFC 2205), incorporated herein by reference. Destination host 120 preferably supports the RSVP receiver host function set forth in RFC 2205; however, source host 110 does not support the RSVP sender host function set forth in RFC 2205. Instead, RSVP-signaled end-to-end QoS provisioning for data flows between source host 110 and destination host 120 is established through the expedient of an RSVP sender host proxy agent implemented on edge switch 140.

In its most basic feature, the RSVP sender host proxy service may be described with reference to Figure 1. RSVP-unaware source host 110 initiates a data flow by transmitting a data packet on the transmission medium interconnecting source host 110 with edge switch 140, the data packet having an address of source host 110 as a source address and an address of destination host 120 as a destination address. Edge switch 140 receives the data packet, determines that the data packet meets RSVP sender host proxy criteria, generates an RSVP Path message in accordance with an RSVP sender host function, modifies certain fields of the RSVP Path message if required in accordance with an RSVP router function, and transmits the RSVP Path message on backbone network 130. The RSVP Path message traverses backbone network 130 and edge switch 160 along a flowpath between source host 110 and destination host 120, whereat certain fields of the message may be modified at each "hop" in accordance with the RSVP router function, and eventually arrives at RSVP-aware destination host 120. Destination host 120, in response to the RSVP Path message, generates an RSVP Resv message requesting a QoS reservation in accordance with the RSVP receiver host function and transmits the RSVP Resv message on the transmission medium interconnecting destination host 120 and edge switch 160. Edge switch 160 receives the RSVP Resv message and, in conjunction with policy server 170 and in accordance with the RSVP router function, determines whether or not to accept the reservation. The RSVP Resv message traverses backbone network 130 and edge switch 140 along the flowpath, whereat it is determined at each "hop" in accordance with the RSVP router function whether to accept the reservation, with edge switch 140 making the determination in conjunction with policy server 150.

Various elaborations of this basic RSVP sender host proxy service are possible as described hereinafter. Nevertheless, at a fundamental level, this basic proxy service, despite its

apparent simplicity, is believed to confer a significant advance over the prior art by expanding the reach of RSVP-signaled QoS provisioning to flows involving source hosts that are RSVP-unaware.

Turning now to Figure 2 a preferred RSVP sender host proxy service will be described in even greater detail by reference to "on switch" processing on edge switch 140. Edge switch 140 has network interfaces 210, 220, 230 and management interface 240 linked by data bus 250. Network interfaces 210, 220, 230 interconnect RSVP-unaware source host 110, switches in backbone network 130 and policy server 150 over different interfaces. Management interface 240 supports various modules, including QoS mapper/classifier 241, QoS manager 242, policy manager 243, QoS driver 244, source learning 245 and RSVP 246. RSVP 246 includes RSVP router agent 247 and RSVP sender host proxy agent 248. Management interface 240 and network interfaces 210, 220, 230 are linked by management bus 260 for transmitting and receiving management information including QoS information for various flows.

Edge switch 140 supports RSVP processing as follows. RSVP message packets received on edge switch 140 are captured off data bus 250 by management interface 140. RSVP message packets are forwarded to RSVP 246 for processing by RSVP routing agent 247 in accordance with the RSVP router function. RSVP router function processing of RSVP Path message packets includes modifying certain message fields as required to indicate limitations and conditions on the ability of switch 140 to deliver QoS services to the flow. RSVP router function processing of RSVP Resv message packets includes determining whether or not to accept requested QoS reservations based on whether switch 140 has sufficient available resources to provide the requested QoS and whether the flows in question are entitled to the requested QoS. The determination of whether or not to accept QoS reservations is made in concert with QoS manager 242 and policy manager 243. Rules defining applicable QoS limitations and conditions are "pulled down" to policy manager 243 from policy server 150 and applied in the determination. RSVP router function forwards RSVP Path message packets, including any modifications, to the "next hops" in the network, and forwards RSVP Resv message packets, including any modifications, to the "previous hops" in the network.

QoS manager 242 facilitates QoS establishment on switch 140 in accordance with accepted QoS reservations. For flows for which reservations have been accepted, QoS manager 242 receives from policy manager 243 QoS policies, divides the QoS policies into flow identifier and QoS parts and forwards the parts to the QoS mapped classifier 241. Mapped classifier 241 associates the flow identifiers with queues supporting the QoS and forwards the associations to QoS driver 244, which establishes flow identifier/queue associations on network interfaces 210, 220, 230 via management bus 260 to implement the QoS policies on switch 140.

In addition to the RSVP processing described above, edge switch 140 supports a novel RSVP sender host proxy function as follows. Data packets received on switch 140 and having unknown source addresses are captured off data bus 250 by management interface 140. Unknown

source address data packets are forwarded to source learning 245 for establishing associations on switch 140 between the source addresses and the network interfaces on which the source addresses arrived. Unknown source address data packets are also forwarded to QoS manager 242 to determine whether the RSVP sender host proxy function is enabled for the sources in question. Where enabled, unknown source address packets are forwarded to RSVP sender host proxy agent 248 for processing in accordance with an RSVP sender host function. RSVP sender host function processing includes generating RSVP Path message packets specifying parameters for the flows in question and forwarding RSVP Path message packets for processing by RSVP routing agent 247 in accordance with the RSVP router function as described earlier.

Turning to Figure 3a, the general format of an RSVP Path message packet is shown. The format and content of such a packet is well known and described in RFC 2205. Generally such a packet generally includes a Layer 2 header 310 followed by a Layer 3 header 320 and RSVP Path message 330. Layer 2 header 310 includes source and destination addressing information. Layer 3 header 320 is generally an IP header including source and destination addressing information and specifying protocol number "46". RSVP Path message 330 includes an RSVP common header identifying the message as a Path message and an RSVP object including the contents of the Path message. The contents of the Path message include a Sender TSPEC describing the flow the sender expects to generate and an ADSPEC. The Sender TSPEC traverses the flowpath from the RSVP sender to the RSVP receiver without modification, whereas the ADSPEC may be modified by switches along the flowpath to indicate the availability of QoS control services and parameters required for QoS control services to operate correctly.

Turning to Figure 3b, the general format of an RSVP Resv message packet is shown. The format and content of such a packet is well known and described in RFC 2205. Generally such a packet generally includes a Layer 2 header 340 followed by a Layer 3 header 350 and RSVP Resv message 360. Layer 2 header 340 includes source and destination addressing information. Layer 3 header 340 is generally an IP header including source and destination addressing information and specifying protocol number "46". The RSVP Path message 350 includes an RSVP common header identifying the message as a Resv message and an RSVP object including the contents of the Resv message. The contents of the Resv message include a requested QoS control service, a Receiver TSPEC describing the flow for which resources should be reserved and, if indicated by the requested QoS control service, a Receiver RSPEC describing the level of service being requested. The contents together form a FLOWSPEC that traverses the flowpath from the RSVP receiver to the RSVP sender and may be modified by switches along the flowpath.

Turning now to Figure 4, a network is shown in which a preferred RSVP receiver host proxy service in accordance with the invention is operative. The network includes an RSVP-unaware destination host 410 having access to backbone network 430 via edge switch 440. Edge switch 440 is coupled to edge switch 460 via one or more core switches (not shown) in backbone

network 430. Edge switch 460 is coupled to RSVP-aware source host 420. Edge switches 440,460 are also coupled to policy servers 450,470, respectively.

Hosts 410, 420 are preferably network end-stations, such as PCs, workstations or servers, having respective network interfaces for packetized communication with other hosts via edge switches 440, 460, respectively. Edge switches 440. 460 are preferably gateway devices. such as hubs, bridges or routers, having a plurality of respective network interfaces for forwarding packetized communications originated by hosts. Policy servers 450, 470 retain quality of service (QoS) rules for application on switches 440, 460, respectively, based on flow characteristics. Hosts 410, 420, switches 440, 460 and policy servers 450, 470 may be interconnected via cables or other transmission media, and may support various protocols, such as Ethernet, IP and ATM. Edge switches 440, 460 preferably support the RSVP router function set forth in RFC 2205. Source host 420 preferably supports the RSVP sender host function set forth in RFC 2205; however, destination host 410 does not support the RSVP receiver host function set forth in RFC 2205. Consequently, end-to-end QoS provisioning for data flows between source host 420 and destination host 410 is established through the expedient of an RSVP receiver host proxy agent implemented on edge switch 440.

In its most basic feature, the RSVP receiver host proxy service may be described with reference to Figure 4. RSVP-aware source host 420 generates in accordance with the RSVP sender host function an RSVP Path message having an address of RSVP-unaware destination host 410 as a destination address and transmits the RSVP Path message on the transmission medium interconnecting source host 420 with switch 460. Switch 460 receives the RSVP Path message, modifies certain fields of the message if required in accordance with the RSVP router function, and transmits the RSVP Path message on backbone network 430. The RSVP Path message traverses switches along the flowpath in backbone network 430 hop-by-hop whereat certain fields of the message may be modified in accordance with the RSVP router function, and eventually arrives at switch 440. Switch 440 modifies certain fields of the message in accordance with the RSVP router function. determines that the RSVP Path message packet meets RSVP receiver host proxy criteria, and generates in response an RSVP Resv message in accordance with the RSVP receiver host function. Switch 440 determines, in conjunction with policy server 450 and in accordance with the RSVP router function, whether to accept the reservation itself prior to transmitting the RSVP Resv message back up the flowpath on backbone network 430. The RSVP Resv message traverses switches in backbone network 430 and switch 460, whereat it is determined hop-by-hop in accordance with the RSVP router function whether to accept the reservation. with switch 460 making the determination in conjunction with policy server 470.

Various elaborations of this basic RSVP receiver host proxy service are possible as described hereinafter. Nevertheless, at a fundamental level, this basic proxy service, despite its apparent simplicity, is believed to confer a significant advance over the prior art by expanding

the reach of RSVP to allow end-to-end QoS provisioning for flows involving a destination host that is RSVP-unaware.

Turning now to Figure 5 a preferred RSVP receiver host proxy service will be described in greater detail by reference to "on switch" processing on edge switch 440. Switch 440 has network interfaces 510, 520, 530 and management interface 540 linked by data bus 550. Network interfaces 510, 520, 530 interconnect destination host 410, switches in backbone network 430 and policy server 450 over different interfaces. Management interface 540 supports various modules, including QoS mapper/classifier 541, QoS manager 542, policy manager 543, QoS driver 544, source learning 545 and RSVP 546. RSVP 546 includes an RSVP router agent 547 and an RSVP receiver host proxy agent 548. Management interface 540 and network interfaces 510, 520, 530 are linked by management bus 560 for transmitting and receiving management information including QoS information for various flows.

Switch 440 supports RSVP processing as follows. RSVP message packets received on switch 440 are captured off data bus 550 by management interface 540. RSVP message packets are forwarded to RSVP 546 for processing by RSVP routing agent 547 in accordance with the RSVP router function, subject to exceptions specified herein. In the case of RSVP Path message packets, RSVP router function processing includes modifying certain fields in the Path message as required to indicate limitations and conditions on the ability of switch 540 to deliver QoS services to the flow. In the case of RSVP Resv message packets, RSVP router function processing includes determining whether or not to accept requested QoS reservations based on whether switch 440 has sufficient available resources to provide the requested QoS and whether the flows in question are entitled to the requested QoS. The determination of whether or not to accept QoS reservations is made in concert with QoS manager 542 and policy manager 543. Rules defining applicable QoS limitations and conditions are "pulled down" to policy manager 543 from policy server 450 and applied in the determination. RSVP router function forwards RSVP Resv message packets, including any modifications, to the "previous hops" in the network. RSVP router function also forwards RSVP Path message packets, including any modifications, to the "next hops" in the network, except where the RSVP receiver host proxy function is enabled for the destinations in question. Where enabled, RSVP Path messages are not forwarded to the "next hops" in the network.

In addition to the RSVP processing described above, switch 440 supports a novel RSVP receiver host proxy function as follows. RSVP Path message packets are forwarded to QoS manager 542 to determine whether the RSVP receiver host proxy function is enabled for the destinations in question. Where enabled, RSVP Path message packets are forwarded to RSVP receiver host proxy agent 548 for processing in accordance with an RSVP receiver host function. RSVP receiver host function includes generating RSVP Resv message packets in response to the

RSVP Path message packets and forwarding the RSVP Resv message packets for processing by RSVP routing agent 547 in accordance with the RSVP router function as described earlier.

In Figure 6, a flow diagram illustrates RSVP packet handling on a switch supporting an RSVP sender host proxy function in accordance with a preferred embodiment of the invention. A packet is received on the switch (610) and a determination is made whether the packet is an RSVP message packet (620). If the packet is an RSVP message packet, the packet is processed in accordance with the RSVP router function (650). If the packet is not an RSVP message packet, a determination is made whether the packet has a source address that is unknown to the switch, indicating a new flow for which a QoS has not yet been provisioned (630). If the packet has an unknown source address, a determination is made whether the RSVP sender host proxy service is enabled for the source (640). If the RSVP sender proxy service is enabled for the source, an RSVP Path message packet is generated (650). The RSVP Path message is processed by the switch in accordance with the RSVP router function (660). If, however, the source address is known to the switch (per the determination in Step 630), or if the RSVP sender host proxy service is not enabled for the source (per the determination in Step 640), RSVP processing of the received packet is terminated.

In Figure 7, a flow diagram illustrates RSVP packet handling on a switch supporting an RSVP receiver host proxy function in accordance with a preferred embodiment of the invention. A packet is received on the switch (710) and a determination is made whether the packet is an RSVP message packet (720). If the packet is an RSVP message packet, a determination is made whether the packet is an RSVP Path message packet (730). If the packet is not an RSVP Path message packet, RSVP processing of the received packet proceeds in accordance with the RSVP router function (740). If the packet is an RSVP Path message packet, however, a determination is made whether the RSVP receiver host proxy service is enabled for the destination (750). If the RSVP receiver host proxy service is not enabled for the destination, RSVP processing of the received packet proceeds in accordance with the RSVP router function (740). If the RSVP receiver host proxy service is enabled for the destination, however, RSVP processing of the received packet proceeds in accordance with the RSVP router function except the Path message is not forwarded by the switch to the "next hop" in the network (760), and an RSVP Resv message packet is generated (770). The RSVP Resv message is processed by the switch in accordance with the RSVP router function (780).

It will be appreciated by those of ordinary skill in the art that the invention can be embodied in other specific forms without departing from the spirit or essential character hereof. For instance, while the illustrated embodiments describe RSVP proxy-signaled end-to-end QoS provisioning for unicast flows between a source host and a single destination host, the invention may be applied to multicast flows between a source host and multiple destination hosts, wherein one or more switches act as RSVP host proxies for the source host and/or one or more of the destination hosts. The present description is therefore considered in all respects illustrative and

not restrictive. The scope of the invention is indicated by the appended claims, and all changes that come within the meaning and range of equivalents thereof are intended to be embraced therein.

We claim:

1. A Resource Reservation Protocol (RSVP) proxy method for a communication network having a plurality of nodes, the method comprising:

generating a data packet on a first node;

transmitting the data packet to a second node;

determining on the second node in response to the data packet whether the second node is an RSVP proxy for the first node;

generating an RSVP Path message in response to the determination; and

transmitting the RSVP Path message to a third node.

2. The method of claim 1, wherein the first node is a host and the second node is a switch.

3. The method of claim 1, wherein the determination is made in accordance with a source address in the packet.

4. A Resource Reservation Protocol (RSVP) proxy method for a communication network having a plurality of nodes, the method comprising:

generating an RSVP Path message on a first node;

transmitting the RSVP Path message to a second node;

determining on the second node in response to the RSVP Path message whether the second node is an RSVP proxy for a third node;

generating an RSVP Resv message in response to the determination; and

transmitting the RSVP Resv message to the first node.

5. The method of claim 4, wherein the first node and the third node are hosts and the second node is a switch.

6. The method of claim 4, wherein the determination is made in accordance with a destination address in the packet.

7. An RSVP proxy method for a communication network having a plurality of hosts and a switch, the method comprising:

transmitting a data packet from a first host to a switch;

originating an RSVP Path message on the switch in response to the data packet;

transmitting the RSVP Path message from the switch to a second host; and

transmitting an RSVP Resv message from the second host to the switch in response to the RSVP Path message.

8. The method according to claim 7, wherein the first host is RSVP-unaware.

9. The method according to claim 7, further comprising reserving resources along a flowpath between the second host and the switch in response to the RSVP Resv message.

10. An RSVP proxy method for a communication network having a plurality of nodes, the method comprising:

transmitting an RSVP Path message from a first host to a switch;

originating an RSVP Resv message on the switch in response to the RSVP Path message;

transmitting the RSVP Resv message from the switch to the first host.

11. The method according to claim 10, wherein the first host is RSVP-unaware.

12. The method according to claim 11, further comprising reserving resources along a flowpath between the first host and the switch in response to the RSVP Resv message.

13. An RSVP proxy service for a communication network, comprising:

a host for transmitting a data packet;

an edge switch for receiving the data packet from the host;

an RSVP host proxy agent on the edge switch for generating and transmitting to a backbone network, in response to the data packet, an RSVP Path message.

14. An RSVP proxy service for a communication network, comprising:

a host for transmitting an RSVP Path message;

an edge switch for receiving the RSVP Path message from a backbone network;

an RSVP host proxy agent on the edge switch for generating and transmitting to the backbone network, in response to the RSVP Path message, an RSVP Resv message.

15. An RSVP proxy service for a communication network, comprising:

a host connected to an edge switch, the edge switch managing the flow of data packets from the host to a backbone network; and

wherein the edge switch receives a data packet from the host and in response generates and transmits an RSVP Path message on the backbone network.

16. An RSVP proxy service for a communication network, comprising:

a host connected to an edge switch, the edge switch managing the flow of data packets from the host to a backbone network; and

wherein the edge switch receives an RSVP Path message destined for the host from the backbone network and in response generates and transmits an RSVP Resv message on the backbone network.

17. An RSVP proxy service for a communication network, comprising:

a first node connected to a second node, the second node providing an interface between the first node and a backbone network; and

wherein the second node receives a data packet from the first node and in response generates and transmits an RSVP Path message on the backbone network.

18. An RSVP proxy service for a communication network, comprising:

a first node connected to a second node, the second node providing an interface between the first node and a backbone network; and

wherein the second node receives an RSVP Path message destined for the first node from the backbone network and in response generates and transmits an RSVP Resv message on the backbone network.

19. A signaling method for establishing an end-to-end Quality of Service (QoS) for a data flow in a communication network utilizing a signaling proxy, the method comprising:

generating a data packet on a first node;

transmitting the data packet to a second node;

determining on the second node in response to the data packet whether the second node is a QoS signaling proxy for the first node;

generating a QoS message in response to the determination; and

transmitting the QoS message to a third node.

20. The method of claim 19, wherein the first node is a host and the second node is a switch.

21. The method of claim 20, wherein the determination is made in accordance with a source address in the packet.

22. The method of claim 20, wherein the QoS message specifies parameters for a data flow.

23. The method of claim 20, wherein the QoS message is modified in route to the third node.

24. A signaling method for establishing an end-to-end Quality of Service (QoS) for a data flow in a communication network utilizing a signaling proxy, the method comprising:

generating a first QoS message on a first node;

transmitting the first QoS message to a second node;

determining on the second node in response to the QoS message whether the second node is a QoS signaling proxy for a third node;

generating a second QoS message in response to the determination; and

transmitting the second QoS message to the first node.

25. The method of claim 24, wherein the first node and the third node are hosts and the second node is a switch.

26. The method of claim 24, wherein the determination is made in accordance with a destination address in the first QoS message.

27. The method of claim 24, wherein the first QoS message specifies parameters for a data flow.

28. The method of claim 24, wherein the first QoS message is modified in route to the second node.

29. The method of claim 24, wherein the second QoS message requests establishment of a QoS for a data flow.

30. The method of claim 24, wherein a QoS is established for a data flow at nodes along a flowpath between the second node and the first node in response to the second QoS message.

31. A service for establishing end-to-end QoS in a communication network, comprising:

a host connected to an edge switch, the edge switch managing the flow of data packets from the host to a backbone network; and

wherein the edge switch receives a data packet from the host and in response generates and transmits a QoS message on the backbone network.

32. The service according to claim 31, wherein the QoS message specifies parameters for a data flow.

33. A service for establishing end-to-end QoS in a communication network, comprising:

a host connected to an edge switch, the edge switch managing the flow of data packets from the host to a backbone network; and

wherein the edge switch receives a first QoS message destined for the host from the backbone network and in response generates and transmits a second QoS message on the backbone network.

34. The service according to claim 33, wherein the first QoS message specifies parameters for a data flow.

35. The service according to claim 33, wherein the second QoS message requests establishment of a QoS for a data flow.

Figure 1

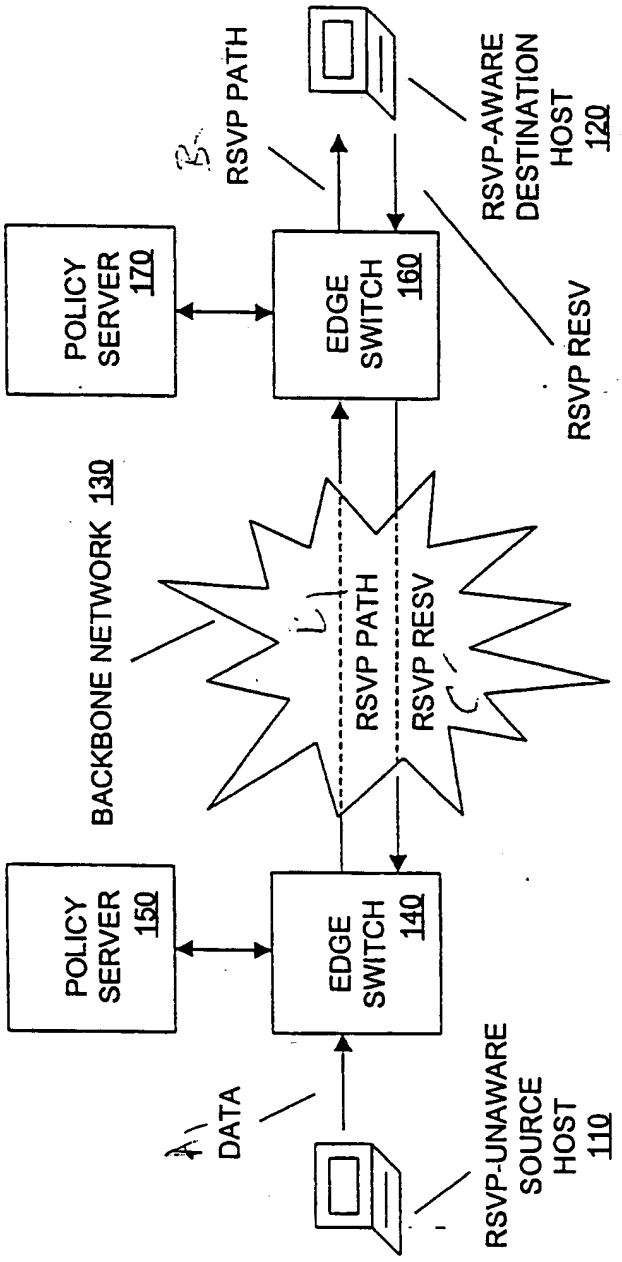

RSVP-UNAWARE SOURCE HOST 110
DATA
POLICY SERVER 150
EDGE SWITCH 140
BACKBONE NETWORK 130
RSVP PATH
RSVP RESV
POLICY SERVER 170
EDGE SWITCH 160
RSVP PATH
RSVP RESV
RSVP-AWARE DESTINATION HOST 120

Figure 2

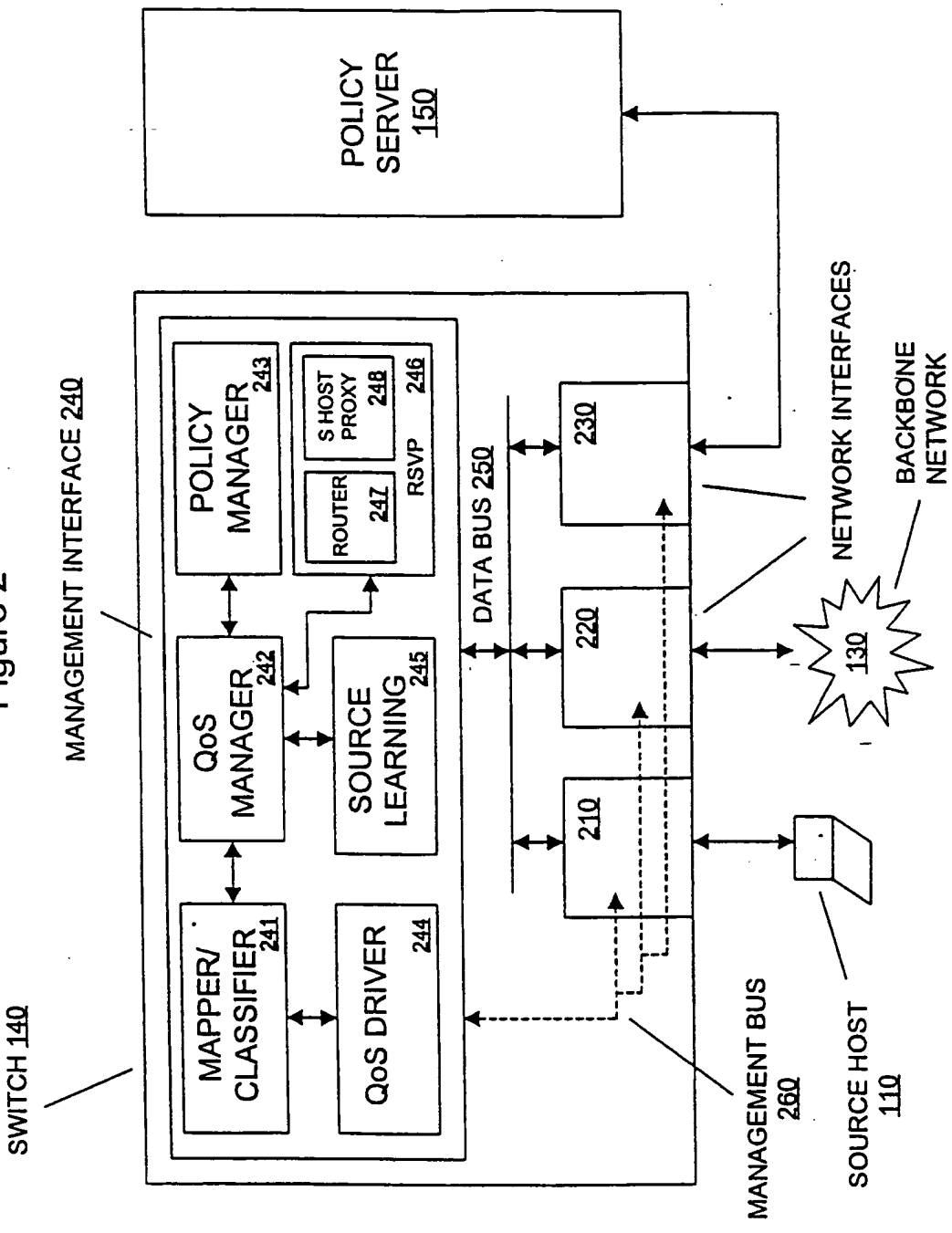

POLICY SERVER 150
MANAGEMENT INTERFACE 240
POLICY MANAGER 243
S HOST PROXY 248
ROUTER 247
RSVP 246
QoS MANAGER 242
SOURCE LEARNING 245
MAPPER/ CLASSIFIER 241
QoS DRIVER 244
DATA BUS 250
230
220
210
NETWORK INTERFACES
BACKBONE NETWORK
130
SWITCH 140
MANAGEMENT BUS 260
SOURCE HOST 110

Figure 3A

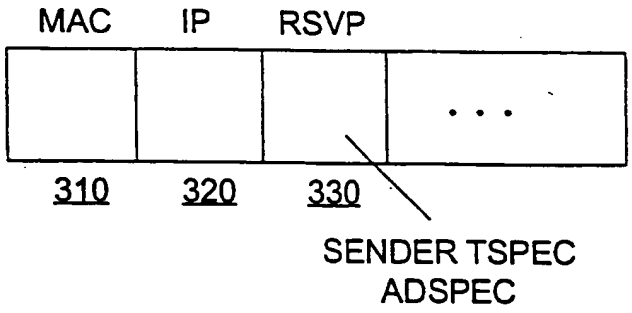
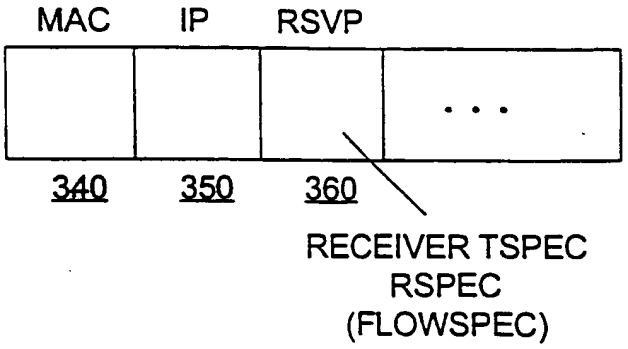


Figure 3B



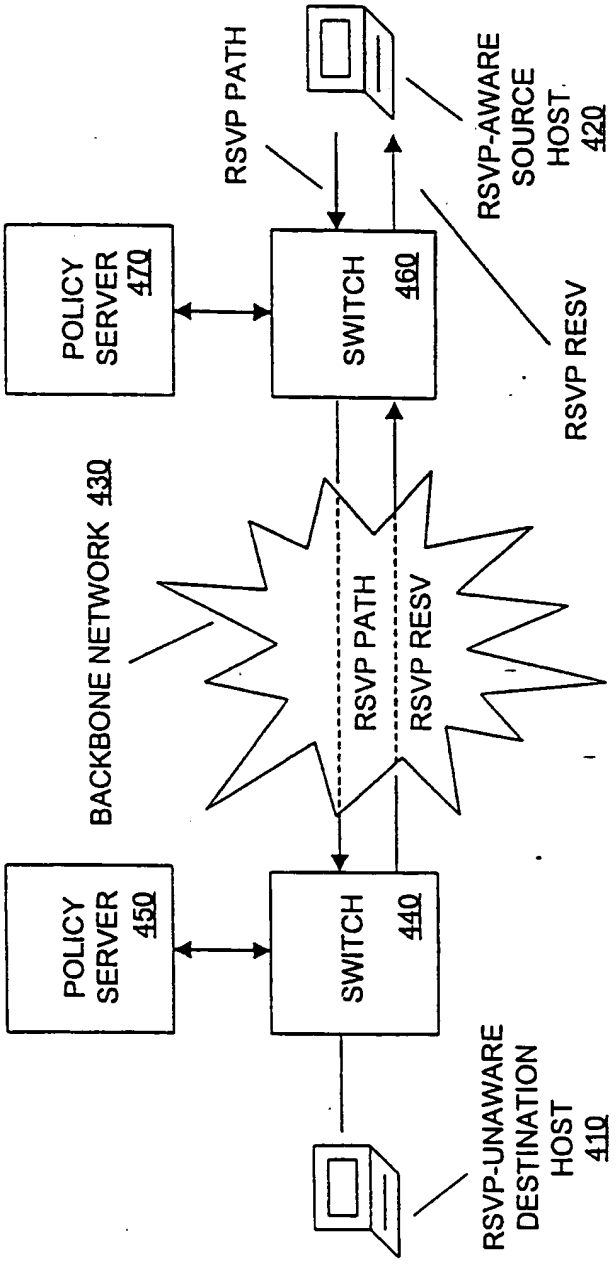
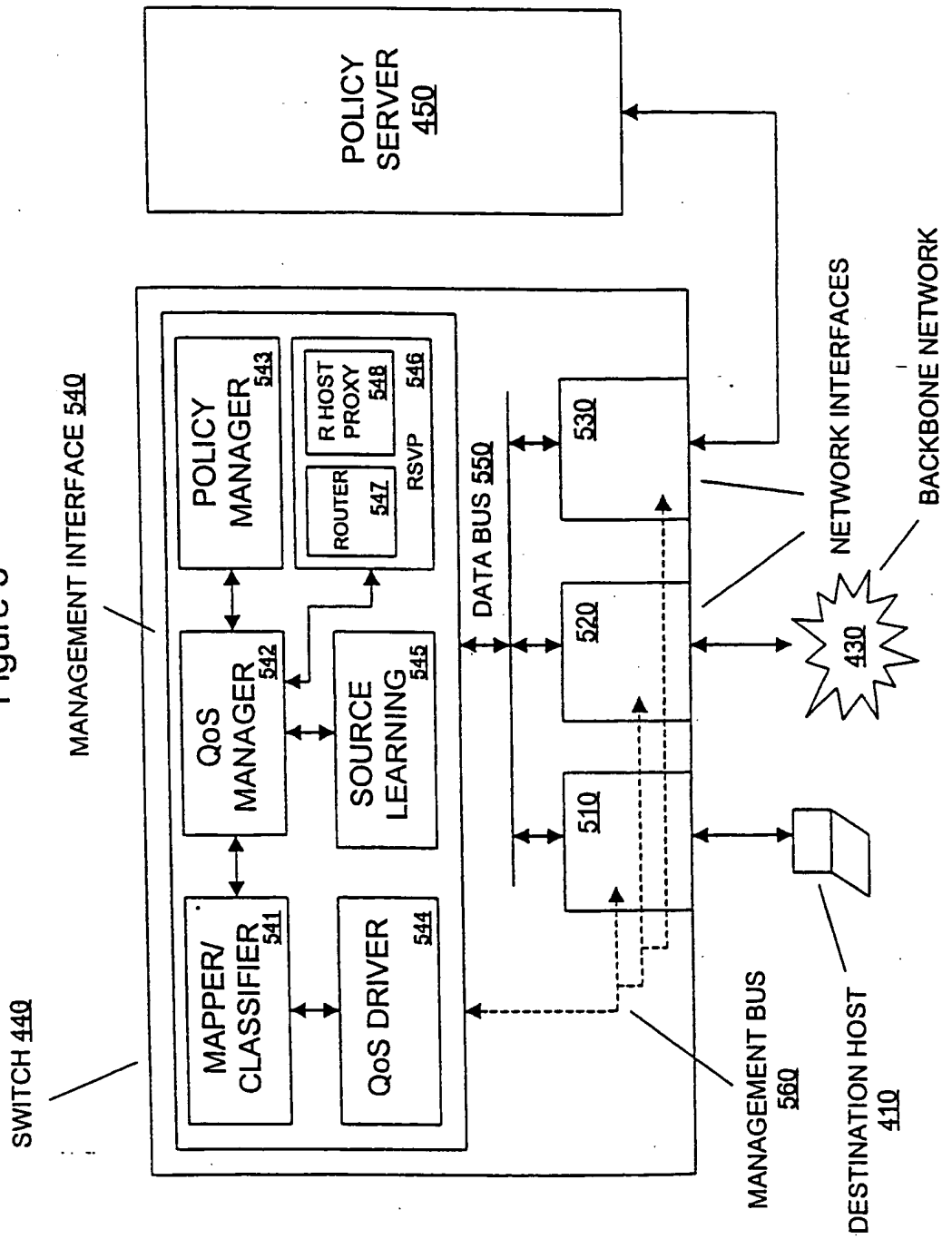

RSVP PATH
RSVP-AWARE SOURCE HOST 420
POLICY SERVER 470
SWITCH 460
RSVP RESV
BACKBONE NETWORK 430
RSVP PATH
RSVP RESV
POLICY SERVER 450
SWITCH 440
RSVP-UNAWARE DESTINATION HOST 410

Figure 4

Figure 5


POLICY SERVER 450
MANAGEMENT INTERFACE 540
POLICY MANAGER 543
R HOST PROXY 548
ROUTER 547
RSVP 546
QoS MANAGER 542
SOURCE LEARNING 545
MAPPER/ CLASSIFIER 541
QoS DRIVER 544
DATA BUS 550
530
520
510
NETWORK INTERFACES
BACKBONE NETWORK
430
SWITCH 440
MANAGEMENT BUS 560
DESTINATION HOST 410

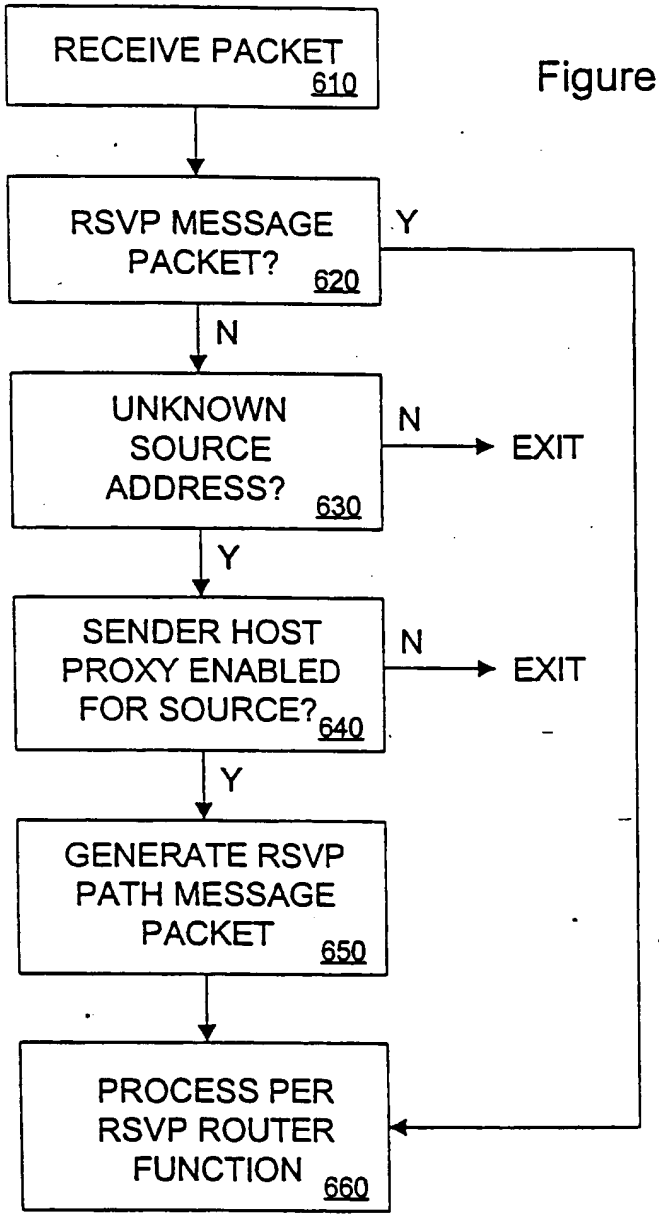

RECEIVE PACKET
610
RSVP MESSAGE PACKET?
620
Y
N
UNKNOWN SOURCE ADDRESS?
630
N
EXIT
Y
SENDER HOST PROXY ENABLED FOR SOURCE?
640
N
EXIT
Y
GENERATE RSVP PATH MESSAGE PACKET
650
PROCESS PER RSVP ROUTER FUNCTION
660

Figure 6

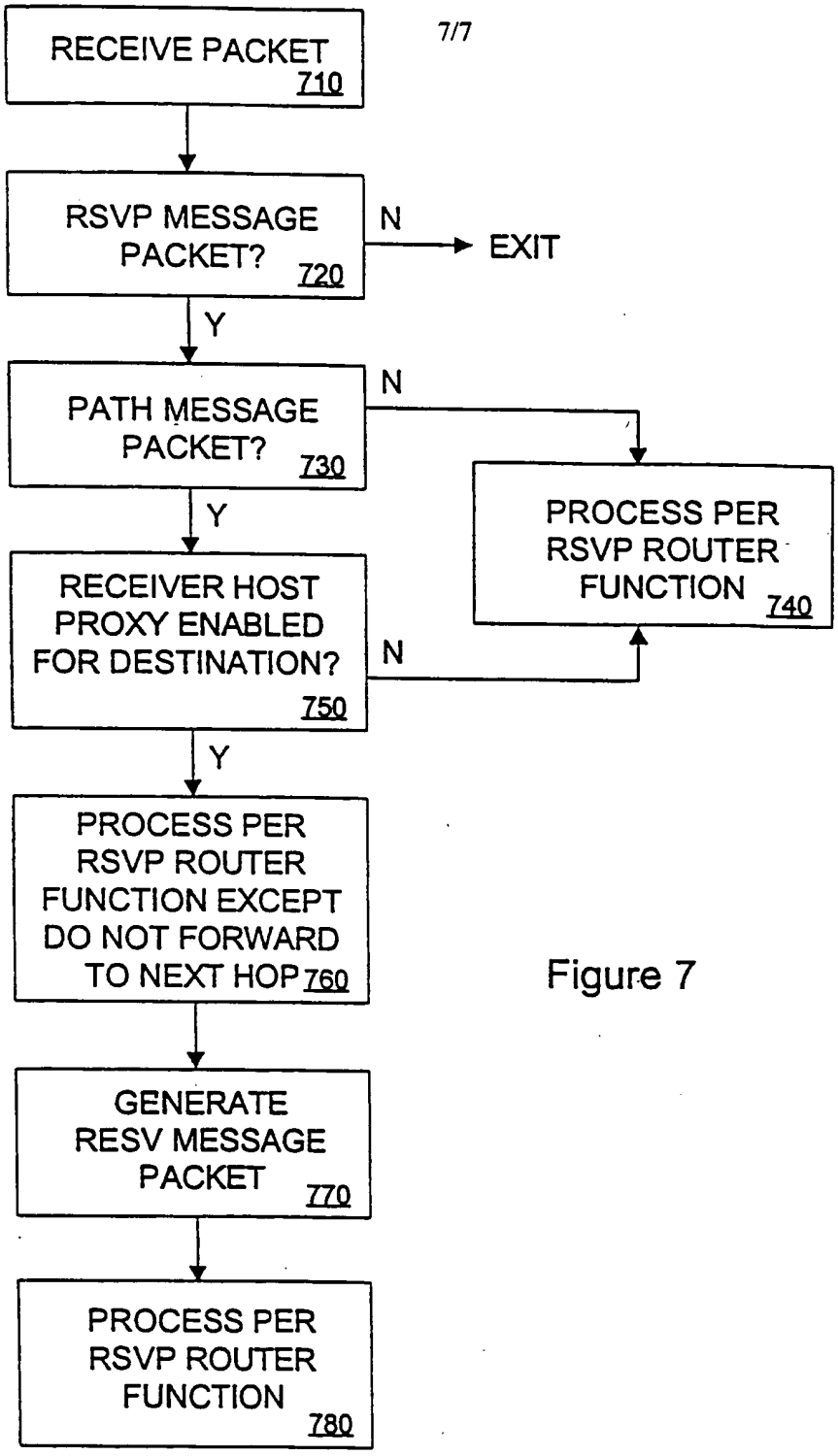

RECEIVE PACKET
710
RSVP MESSAGE PACKET?
720
N
EXIT
Y
PATH MESSAGE PACKET?
730
N
Y
PROCESS PER RSVP ROUTER FUNCTION
740
RECEIVER HOST PROXY ENABLED FOR DESTINATION?
750
N
Y
PROCESS PER RSVP ROUTER FUNCTION EXCEPT DO NOT FORWARD TO NEXT HOP
760
GENERATE RESV MESSAGE PACKET
770
PROCESS PER RSVP ROUTER FUNCTION
780

Figure 7